January 19, 2007

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, NW
Washington, DC 20580
Taskforcecomments@idtheft.gov

Re: Comments to Identity Theft Task Force, P065410

To Whom It May Concern:

The National Business Coalition on E-Commerce and Privacy appreciates the opportunity to provide comments.

The National Business Coalition on E-Commerce and Privacy (the "Coalition"), founded seven years ago, is a diversified organization of 17 brand name U.S. companies (and three industry associations) devoted to balanced domestic and international policy in electronic commerce and privacy. Since its inception in February 2000, the Coalition has played a significant role in helping shape federal legislation on these issues, and it continues to actively participate in the ongoing Congressional consideration of proposed legislation regarding identity theft, data security and notification of security breaches, online privacy, spam and spyware, among other e-commerce and privacy issues. In the course of these efforts, the Coalition has provided Congressional testimony, as well as model legislation, commentary on draft legislative language, and other assistance to Members of Congress and their staff involved in the drafting and consideration of federal legislation to address identity theft and data security breaches.

EXECUTIVE SUMMARY

This Executive Summary of our detailed comments that follow is intended to highlight for the President's Identity Theft Task Force, in a single place, our key recommendations with respect to the specific questions on which it has sought public comment. In addition, this summary discusses a fundamental question applicable to all of the Task Force's questions – what does the Task Force mean by the term "identity theft"? Because the Task Force did not detail its definition, nor ask about it in any of the enumerated questions, this summary provides our views on this question as well.

A. Definition of Identity Theft

1. Introduction

Identity theft is a very serious problem – an insidious crime that often leaves victims' credit histories in shambles. If we are to reduce it, industry, government, law enforcement and consumers all have a role to play. There is some heartening news, though, and we can now see

that efforts by industry, government, law enforcement and consumers are starting to have an effect.

But in order to accurately discuss "identity theft" at all, or to provide meaningful comments to the Task Force on recommendations to reduce it, we must be absolutely clear at the outset about what we mean by the term "identity theft." Unfortunately, the federal government, law enforcement, and industry – not to mention the national media that annually publishes thousands of articles on the subject – are not always clear about what is, and what is not, "identity theft." If policy makers cannot agree on one definition for the purpose of discussing both government and industry methods of addressing the problem, then they risk developing and implementing ineffective solutions, and that would be the true tragedy.

That is why the President's Identity Theft Task Force has such a unique opportunity today – it can help correct the mistakes of the past, and in so doing, unify both public and private efforts to combat this crime. We also continue to offer the Task Force our assistance, based on years of working on this issue with Congress, and in drafting recommendations that would be most effective in addressing identity theft. However, early drafts of the Task Force's proposed recommendations to the President have shown that it may endorse a definition of identity theft that we believe is over-broad and far different from what both consumers and industry commonly understand it to be.

The Coalition therefore respectfully submits to the Task Force that we believe its continued adherence to its previous approach to defining this crime may only perpetuate confusion among consumers, as well as the continued advancement in Congress of legislation insufficiently tailored to address the crime we all wish to eradicate.

In this executive summary of our comments, then, we offer our views on a definition of identity theft that is supported by existing federal criminal law, and that would fulfill the President's goal when he set out to create a Task Force to recommend solutions to the true crime of identity theft. We also recommend in this summary, as well as in the specific comments that follow, that the Task Force adopt a definition of identity theft that is consistent with existing federal law as well as with what both industry and much of academia call "true" identity theft.

2. "True" Identity Theft vs. Credit Card Fraud

Identity theft is commonly understood today, by consumers and industry alike, to be the crime in which a sufficient combination of a victim's identifying information (e.g., name, address, social security number, bank account numbers, etc.) is stolen and used to fraudulently open new accounts in his or her name. Typically, these are credit-based accounts, so the criminal can withdraw money or make purchases of goods or services that will be charged to these new accounts, and therefore to the victim. All too often, the address (or e-mail for paperless statements) have also conveniently been altered so as not to alert the victim that a new account has been opened. As a consequence, victims of this crime are typically unaware what has occurred until the damage is complete, and then they also must spend enormous amounts of time restoring their good name and credit.

This crime of identity theft, then, or "true" identity theft as some articles have recently characterized it, is distinguishable from other types of fraud that may involve customer information but that do not result in the substantial social and economic costs associated with "true" identity theft. For example, losses due to credit card fraud – purchases made using a stolen credit card numbers – are generally borne by the credit card issuing banks and networks, and not consumers. In addition, there is no assumption of the victim's identity. While this crime is significant, to be sure, it usually does not have the recurring impact that "true" identity theft has on consumers, businesses, and the economy as a whole. It is not, simply stated, "true" identity theft, and different solutions are often needed to address these distinctly different crimes.

Additionally, government and industry have worked together for years to address the crime of credit card fraud and to protect consumers from losses that may result from it. These initiatives – from caps on consumer losses to the development of "neural networks" by financial institutions to flag suspicious credit card activity – have served the American public well by helping reduce this crime and eliminating virtually any risk of loss by consumers whenever their credit card numbers are fraudulently used. For these reasons, credit card fraud has been distinguished in federal criminal law from "true" identity theft (*see* sections 1028 and 1029 of title 18 of the U.S. Code). The Coalition therefore urges the Task Force to include in its recommendations a request that Congress devise a new definition of identity theft that would accurately address "true" identity theft.

An additional concern of the Coalition highlighted in the specific comments that follow is related. For example, we respectfully submit that the public interest is not well served when the information provided to consumers by the government about identity theft is imprecise and potentially misleading. In research released to the public last year, Javelin Strategy and Research found that only 6% of identity theft incidents actually occur as a result of data security breaches, and that thefts by those known to the victim (such as relatives, co-workers, home contractors and other acquaintances) results in identity theft incidents 15% of the time, or more than twice the rate of data security breaches. The government's practice of defining identity theft as broadly as possible effectively means that nearly all risks of fraud that involve some kind of information about a consumer are lumped together statistically as "identity theft." Given the extraordinary differences in the impact such crimes have on their victims – as noted above, with respect to "true" identity theft versus credit card fraud – such a broad definition of identity theft distorts the true nature of the crime and potentially misleads consumers. In fact, as Javelin found, such broad terms and statistics are encouraging consumers to expend financial resources, quite apart from the emotional cost, that are unnecessary when the risk of "true" identity theft is virtually nonexistent.

3. Definition of Identity Theft Under FCRA

It has been said that the Fair Credit Reporting Act (FCRA) dictates the FTC's current rule on the definition of identity theft. The FTC's rule (16 CFR 603.2) defines "identity theft" as "a fraud committed *or attempted* using the identifying information of another person without authority" *(emphasis added)*, and "identifying information" is very broadly defined to include a wide range of information. The Task Force should be aware, however, that this definition was created for a very specific purpose under FCRA and that it is arguably unsuitable for broader

application. Specifically, this definition was created for the purpose of determining circumstances in which consumers would be entitled to place an identity theft report with a credit reporting agency about an identity theft crime in order to establish a permanent fraud alert on his or her credit file, or otherwise block information from appearing in credit reports that may be fraudulent (and results from identity theft). In these circumstances, defining the term "identity theft report" broadly enough to capture attempted crimes so that consumers may take actions with credit reporting agencies makes sense – but taking that same definition and using it in a very different context (i.e., defining the crime for purposes of a federal criminal statute) is a substantial over-reach. In fact, it is important to note that the word "attempt does not appear in the statute enacted by Congress authorizing the FTC to define the term "identity theft" for these specific purposes, the Fair and Accurate Credit Transaction Act (FACT Act, section 603(q)(3)). Rather, it is a term that was added in a specific FTC rulemaking on that definition. We therefore urge that the Task Force not simply presume that the definition of "identity theft" in 16 CFR 603.2 is relevant or useful as a proxy for a definition of the crime of "true" identity theft that the President has asked the Task Force to address.

Finally, it is worth noting that the use of this existing definition by the FTC for purposes of compiling statistics on identity theft has resulted in vast statistical differences between the FTC's accounting and that of other agencies and departments of the federal government. A recent article by Fred Cate, a well-published and respected academic on privacy and security issues, pointed out that the FTC's assessment of the number of incidents of identity theft (based on their definition) was nearly twenty times higher than other assessments based on a definition of "true" identity theft.

B. Federal Legislation Regarding Data Security and Breach Notification

The Coalition continues to believe in a straightforward set of core principles that should be embodied in any federal data security legislation that would create both data security safeguards as well as breach notification standards applicable to all businesses operating in the United States. The four core principles we have consistently urged Congress to embrace, and that we now recommend for consideration by the Task Force, in any such proposed data security legislation are that it should: 1) create uniform national standards for consumers and businesses alike; 2) promote a consistent, high level of security for sensitive customer information across all industries; 3) ensure that consumers are provided notice of data security breaches when necessary to protect themselves but will not be overburdened with government-required data breach notices when they are not actually at a significant risk of suffering identity theft as a result of a breach in security; and 4) establish an effective, multi-layered federal enforcement regime through functional federal regulator enforcement of the law for regulated businesses and FTC enforcement of the law for businesses not subject to functional regulation.

These principles, and the provisions we recommend by which to achieve them, are discussed in greater detail in the specific comments to the Task Force's questions, primarily in section I.3 and I.4. They are also augmented by our views on other key provisions defining the scope of federal data security legislative proposals, such as the definitions of covered entities, covered data, and identity theft itself (as discussed above). For purposes of this executive

summary, however, we briefly highlight the four key principles and considerations regarding the scope of proposed legislation below.

1. Federal Preemption of State Laws

To achieve uniform national standards for consumers and businesses alike, the Coalition strongly supports the enactment of a federal law that is effectively preemptive of the numerous and varying data security breach notification laws that have been enacted by the states (to date, numbering 35). Absent such federal preemption, federal legislation on the subject is valueless, as it simply would become potentially the 51st law on the subject (if all states were to act). It would also unnecessarily raise compliance costs, with no corresponding benefit for consumers. We therefore urge the Task Force to make federal preemption of state laws an indispensable element of any of its proposed recommendations regarding federal data security safeguards and/or federal breach notification legislation.

2. Affirmative Obligations for Industry to Protect Sensitive Data

To promote a consistent, high level of security for sensitive customer information across all industries in America, the Coalition recommends that the Task Force endorse enactment of a federal law that would create a uniform set of data security safeguards for businesses, regardless of industry. The Coalition recommends, as further discussed in our comments, that the Task Force consider the flexible approach taken by existing federal data security safeguards, statutes and regulations, such as those contained in the Gramm-Leach-Bliley Act and the FTC Safeguards Rule, when developing any recommended standards for industries not currently required by law to provide for the security of customer data. Similar to many state laws and all of the key federal data security bills reported from committees in the 109th Congress, any such legislation should also provide adequate "safe harbors" for those entities in compliance with existing federal data security provisions enforceable by federal functional regulators and/or the FTC.[1]

3. Risk-Based Breach Notification Trigger

To ensure that consumers are provided notice of data security breaches when necessary to protect themselves, but will not be overburdened with government-required data breach notices when they are not actually at risk of suffering identity theft as a result of a breach, the Coalition recommends the Task Force adopt the standard already advocated by the FTC in Congressional hearings – that notification of a data breach must be provided only to individuals who face "a significant risk of identity theft" as a result. As the FTC has wisely recognized, requiring notices to be sent when there is no likelihood of harm will likely desensitize consumers to situations that may later occur where they indeed do face a risk of becoming a victim of identity theft. Additionally, as the Javelin study and recent press accounts have noted, over-notification of consumers is already taking place due to businesses' compliance with numerous state data breach laws that do not have a risk-based notification standard. In addition, Javelin found that such over-notification of security breaches has exaggerated the prevalence of "true" identity theft, unnecessarily alarmed consumers, and encouraged Americans to expend time and money

[1] As used throughout these comments, the term "safe harbor" means that an entity's compliance with an existing federal law's security standards would be deemed to be compliance with any new law's standards.

to protect themselves from harm that actually does not exist. A risk-based notification standard is therefore necessary to prevent the corresponding harm to consumers presented by over-notification of security breaches that consumers are currently experiencing.

4. Federal Enforcement Regime

To establish an effective, multi-layered federal enforcement regime of any proposed legislation, the Coalition recommends that the Task Force endorse a regime that would provide for enforcement of federal laws at the federal level – specifically, a regime where financial institutions are under the enforcement authority of their functional federal regulator and the FTC enforces the law for non-functionally regulated companies. Additionally, the Coalition recommends that such legislation not be enforceable by state attorneys general, as such enforcement within states may lead to uneven application and interpretations of the federal law's provisions based simply on geographic location. Rather, we recommend that the Task Force consider the use of U.S. Attorney Offices to enforce the law under the direction of the U.S. Attorney General and the Department of Justice. Not only do U.S. Attorneys outnumber state attorneys general – thereby providing greater coverage of the United States on a per capita basis – but they also have the benefit of being federal enforcement authorities under the direction of the U.S. Attorney General, who is better situated to enforce any federal data security law more evenly throughout the United States than would 50 different state attorneys general. Finally, the Coalition recommends that the Task Force reject private rights of action as a mechanism to enforce data security safeguards and breach notification legislation, similar to the majority of the congressional committees that reported federal data security bills in the 109th Congress. As FTC Chairman Majoras has testified, no data security solution is perfect, and data security breaches are inevitable despite the best efforts of industry or government to protect against it. That reality means that law enforcement must exercise discretion, looking at the facts of each case, in order to determine when a violation has truly occurred.

5. Proper Scope of Proposed Law

As detailed in the specific comments to the Task Force's questions below, the Coalition recommends that the Task Force consider the following key provisions that circumscribe the proper scope of any proposed data security safeguards and/or breach notification legislation.

Focus on Identity Theft and Data Security

Primarily, the Coalition respectfully suggests that the Task Force limit the scope of any of its proposed legislative recommendations to the issue of "true" identity theft (as discussed above), and that this issue not be diluted by proposals on important but nonetheless unrelated issues, such as spyware and data privacy concerns (including regulations regarding the use and sharing of information by individual companies). Those subject areas, while tangentially related, should be addressed by separate legislative proposals from the federal government, and should not be part of any recommended legislation proposed by the Task Force given its overarching mandate to advise the President on identity theft.

Harmonization with Existing Federal Laws

Secondly, to ensure that all industries are covered by fundamental data security and breach notification requirements, the Coalition recommends that the Task Force's strategic plan proposes policies that recognize that federal data security laws and regulations already exist for certain industry segments (including entities subject to financial and health care privacy and security laws), and that the Task Force should not recommend imposing new and unnecessary burdens on those entities that simply duplicate the compliance requirements without adding any corresponding additional benefits for consumers. The Task Force should therefore recommend that entities subject to and in compliance with existing data security laws must be afforded a safe harbor for their compliance with those laws in any new legislation that is proposed.

Definition of Covered Data

Lastly, the Coalition urges the Task Force to pay great attention to the specific definitions of key terms in any legislative proposals it may recommend, in particular what the Task Force considers to be the types of "covered data" that would be protected by any safeguards standards and also would be subject to notification following a breach in security involving that data. Our specific comments to the Task Force's questions (in section I.4) provide additional detail on how such term could be clearly defined, and our response includes specific textual references to state statutory language that we believe has worked effectively to define the proper scope of data coverage. Essential to our views of the proper scope of covered data are three key recommendations we make to the Task Force: 1) follow the example of nearly all state data security laws to ensure that covered data is limited to the types of sensitive personal information that can actually be used to commit identity theft (e.g., an SSN alone would be insufficient); 2) adopt the standard in any legislative proposals, as many states have done, that consumer notification is not required when covered data has been rendered unreadable or otherwise unusable, either through encryption, redaction, truncation or other equally effective methods; and 3) recognizing that federal, state and local governments make publicly available personal information of consumers on a daily basis, adopt the standard similar to many state laws that does not require notification of a breach of security of such data as it cannot cause any risk of harm greater than that which already exists by government's own publication of it.

COMMENTS TO SPECIFIC QUESTIONS OF TASK FORCE

I. MAINTAINING SECURITY OF CONSUMER DATA

The National Business Coalition on E-Commerce and Privacy provides the following comments in response to the specific questions asked by the Task Force. However, we have also included, in Section I.6 below, entitled "Government Receipt of Technologically Secured Data," additional comment on an important issue that was not the subject of any specific question by the Task Force.

1. Government Use of SSNs

Social Security Numbers ("SSNs") are the only unique identifier that follows a person throughout life. As such, they are also the most effective data elements for use by federal, state, and local governments (not to mention private entities as well) for the purpose of ensuring database accuracy. They are critical to the authentication of the identity of a particular individual and/or determining an individual's current location for a variety of legitimate government purposes.

For example, SSNs are an integral part of the Internal Revenue Service and Social Security systems, as the SSN is the key data element used for the accurate collection of federal and state taxes and the provision of Social Security benefits. In fact, at the federal level alone, SSNs are regularly used for necessary operations of the Department of Justice (including the FBI), the Department of Homeland Security (including Customs and the Transportation Security Administration), the Department of Health and Human Services, the Securities Exchange Commission, the Central Intelligence Agency, along with other agencies and departments of government. Law enforcement use of SSNs routinely go beyond addressing homeland security concerns, as SSNs enable a variety of commonplace law enforcement tools, such as locating non-custodial delinquent parents for the purpose of enforcing child support payments. SSNs are also used by state and local government entities to enforce student loan repayment, as well as to verify identities for a variety of other legitimate purposes at the state and local level.

Therefore, an outright prohibition on the use by government of SSNs would have a devastating effect on government's day-to-day responsibilities. Such a prohibition would not only create confusion by making it more difficult for government entities to authenticate the identities of residents, but also such action would exacerbate the problem of identity theft by eliminating one of the most effective tools to thwart identity theft (properly authenticated SSNs). Short of a prohibition on government use of SSNs, however, there are many common-sense steps that could be recommended by the Task Force to increase protection for SSNs.

One such step would be for the Task Force to recommend that SSNs be prohibited from being displayed on government forms or records that are publicly available, including driver's licenses, state identification cards, tax forms, government checks, and deeds. Federal legislation regarding the display of SSNs has been considered in Congress for years, and various proposals have already had the benefit of being vetted by government and industry alike. We would urge that the Task Force consider recommending that federal government departments and agencies that rely on SSNs continue to work with industry to shape legislation that would establish limits on the unnecessary display of SSNs.

An additional step government could undertake would be to develop a more comprehensive record of government utilization of SSNs that would serve as a basis for analyzing uses that may be reduced or eliminated. While we are concerned with the prohibition of *necessary* government uses of SSNs, the Coalition supports the Task Force's suggested policy recommendation to eliminate *unnecessary* uses of SSNs by federal government agencies and departments. We agree, for example, that there are instances in which SSNs are currently collected from consumers for federal government uses, but the SSN is not actually necessary to

achieve the particular purpose for which it was collected. Similarly, most companies approaching the issue of SSN remediation have made the question of whether an SSN is actually needed for certain business applications a major focus of their efforts to reduce risk.

However, before discussing which government uses of SSNs are *unnecessary*, we urge the Task Force to recommend to the President that the federal government survey the uses of SSNs employed within government, including the potential impact on the government and the public of eliminating any one of them. Given the broad use of SSNs across federal departments and agencies (as noted in the list above), we also suggest that the Task Force recommend that those agencies, and any others it believes depend on such SSNs, be responsible for conducting this multi-agency impact analysis. We further recommend that the study not be solely the work of any one agency (particularly one that does not use SSNs extensively and may underappreciate their importance to the proper functioning of government). Such a study should also involve the private sector to ensure that there is sufficient understanding of how the private sector provides SSNs to the government and for what purposes. Upon completion of the study and impact analysis, the government will be in a better position to determine which current government uses of SSNs are necessary and which are not. Where unnecessary for a legitimate government function, consumers should not be required to provide SSNs to the government, and alternative *methods* of achieving the government purpose (and not necessarily alternative *identification numbers* for the SSN) should be considered to accomplish the government purpose.

While the Task Force seeks input on "alternatives" to government uses of SSNs, the truth is that, for many necessary government functions, there is simply no viable substitute identification number for the SSN. Any potential alternative unique identifier, to be remotely useful to governments in performing many of their necessary functions, would need to have essentially the same principal characteristics of the SSN – an identifier that is unique to one individual through that individual's life. If such an alternative were developed for the purposes of being utilized as a replacement identification number to the SSN, the costs of converting all current government records to the alternative number would be overwhelming. Moreover, such an alternative would not resolve the current concerns about SSN use for identity theft purposes. Rather, the alternative identifier would simply become the "new" SSN, and thus a new target for identity thieves.

We recommend that the Task Force therefore focus its efforts on the real and addressable problem at hand – maintaining the *security* of SSN use and eliminating the unnecessary *display* of the numbers required by government. Additionally, we recommend that the Task Force promote a government-wide study and impact analysis of reducing current uses of the SSN and that the Task Force caution against reducing the use of SSNs where such use is serving legitimate and, indeed, vital government interests in authenticating and locating citizens for either the distribution of benefits, enforcement of law, or other acceptable practices. It may also be worth the Task Force's consideration and acknowledgement in its recommendations to the President that government use of SSNs to authenticate identities and locate individuals already contributes to the reduction and prevention of identity theft and other fraudulent acts upon the government. In conclusion, we believe that government uses of SSNs alone (without further consideration of the context in which those uses occur) should not be readily dismissed by the

Task Force nor considered unnecessary without further study and demonstration of alternative methods that may be employed to achieve a government function at a similar cost to the public.

2. Comprehensive Record on Private Sector Use of SSNs

Similar to government uses of SSNs (see comment I.1), the SSN is essential for private industries as well, in order to access credit records, verify identities and prevent fraud. Addresses, names, and phone numbers are changed millions of times per year, and multiple individuals commonly share the same address (often those who are unrelated). Additionally, individuals often vary the use of their name by using nicknames or by including (or not) a middle name or middle initial, and multiple phonetic spellings of the same name are common place among persons of certain cultures. In this ever-changing landscape of names and addresses for the same individuals, the only effective and unique data element that does not typically change over the course of an individual's life is the SSN. Thus, SSNs are integral to resolving and preventing the problem of true identity theft by providing a vital means to authenticate whether an individual is who he/she claims to be. Unduly restricting or prohibiting access to SSNs will therefore severely disrupt numerous commercial transactions, not to mention law enforcement activities, and would exacerbate identity theft by essentially eliminating the most effective identification verification tool available to American industry.

While the Task Force should not recommend eliminating the commercial *use* of SSNs altogether, we believe it should support reasonable restrictions on the *display* and public *availability* of SSNs by the private sector that can be readily implemented and supported by industry. One approach that has been embodied in federal legislation introduced in previous Congresses has been to prohibit the intentional provision of SSNs, through the online or offline display, or transfer or sale of the numbers, to the general public. For example, such legislation could not only prohibit SSNs from being displayed on the Internet, but also on any form of membership card, employee badge, or other identification card that may be visible to other individuals. Additionally, and apart from authentication purposes for commercial transactions, private entities could be prohibited from requiring a consumer to use his or her SSN as a "password" for access to goods or services.

However, reasonable access to, and use, of SSNs by the private sector can and should be maintained for legitimate purposes, including access to credit, fraud detection and prevention, employment security and screening, "business-to-business" transactions (particularly for small businesses), and investigating insurance fraud and similar crimes. SSNs are a critical element of an individual's credit report, the accuracy of which is important both to consumers and businesses. Utilizing SSNs for this purpose enables companies to accurately identify an individual seeking credit and perform a risk assessment on that individual for credit purposes,. Legitimate uses of the full SSN in business-to-business or business-to-government transactions should be preserved as permitted under the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act (GLBA) – particularly, the purposes identified in Title V, Section 502(e) of GLBA – and as necessary:

- to identify or locate missing and abducted children, witnesses, criminals and fugitives, parties to lawsuits, parents delinquent in child support payments, organ and bone marrow donors, pension fund beneficiaries, and missing heirs;

- for national intelligence purposes;

- for identity verification; and

- for database cross-matching activities to ensure data accuracy.

Additionally, SSNs are of critical importance to financial institutions' compliance efforts with respect to national security and anti-money laundering laws. For example, section 326 of the USA PATRIOT Act requires financial institutions to implement a customer identification program to verify the identities of customers opening new accounts. Identity verification is also a critical component of export controls and defense contracting requirements. Section 103.121 of the Bank Secrecy Act regulations require, for example, that financial institutions:

- implement a written risk-based customer identification program;

- maintain records, including customer information, and methods used to verify customers' identities; and

- compare the names of new customers against government lists of known or suspected terrorists or terrorist organizations when such lists are provided by their federal regulator.

It is critical, therefore, that any government reduction in use of SSNs be harmonized with existing federal laws so that private sector entities are not faced with conflicting federal requirements regarding private sector collection and use of SSNs – a framework in which industries may literally find it impossible to comply with all federal SSN regulations due to their conflicting nature. For these reasons, we urge the Task Force to recommend that the federal government initiate a comprehensive survey and study of private sector uses of SSNs – including all of those required in order to comply with federal law – before making any specific policy recommendations regarding private sector entities' reduction or elimination of any one of such uses.

We also suggest that such a study include an evaluation of the *societal costs* involved in eliminating or reducing the legitimate current uses of SSNs, including the potentially enormous cost of replacing the use of the SSN with any alternative identification number. (As discussed in comment I.1 above, however, we believe that any potential alternative unique identifier to the SSN – none which is readily and broadly available to industry today – would need to have essentially the same principal characteristics of an SSN, and ultimately would fail to resolve the current concerns about SSN use for identity theft purposes but simply become the "new" SSN for thieves to target). Additionally, we recommend that any study conducted on private sector use of SSNs include an analysis of the *benefits to consumers* of the legitimate use of SSNs, both by government and private sector entities, and an analysis of the issues and costs (including any

unfunded mandates on industry) that would be associated with requiring the redaction or truncation of SSNs in public records made available by federal, state and local governments.

As we similarly suggested with respect to a study of government uses of SSNs (in comment I.1), we urge the Task Force to recommend that any private sector study of SSN uses be, at a minimum, a multi-agency endeavor, and in this instance, one that involves all functional regulators that have jurisdiction over commercial entities and their use of customer data, including SSNs. For example, such a study should be jointly conducted jointly by the Department of Treasury, the Federal Reserve Board, the Federal Housing Finance Board, Federal Deposit Insurance Corporation, the Health and Human Services Department, the Internal Revenue Service, the Office of the Comptroller of the Currency, the Office of Federal Housing Enterprise Oversight, the Office of Thrift Supervision, and Securities and Exchange Commission, as well as any other agencies or departments of the federal government that review commercial uses of SSNs.

3. National Data Security Standards

National data security standards already exist in certain industry sectors. For example, under GLBA and its implementing regulations and interagency guidance, "financial institutions" within the jurisdiction of the federal banking regulators are required to safeguard customer information, have a response program in the event sensitive customer is compromised, and to provide notification to customers if warranted. Additionally, the Federal Trade Commission (FTC) ordered and enforces the "Safeguards Rule," which imposes similar requirements on entities that qualify as "financial institutions" under GLBA but that are not otherwise regulated by the federal banking regulators.

We recommend that where the federal functional regulators of various industries have already undertaken significant efforts to establish regulations and guidance on commercial entities' data security and breach notification policies and procedures, the Task Force should not now consider recommending new and potentially burdensome compliance requirements that may be in conflict with, or duplicative of, existing data security regulations. Rather, the Task Force should focus its efforts on ensuring the national and uniform application of data security standards across industries, so that companies and other organizations maintaining sensitive consumer data that are not covered by existing federal data security requirements would be subject to standards similar to those currently in existence.

The Task Force should also recognize the extensive experience of both government and private industry in data security matters, as these issues are simply not *new* policy issues despite the recent surge in press reports covering data security breaches. The Task Force, therefore, has the benefit of examining what has been required federally before and what has proven to be successful in establishing standards that are flexible and able to be implemented by industry to effectively ensure the security of sensitive consumer data. We provide here a very brief summary of existing federal requirements, all of which we recommend the Task Force review in considering the adoption of similar national, uniform data security standards.

Under GLBA and the FTC's Safeguards Rule, covered entities must ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to, or use of, such records or information that could result in substantial harm or inconvenience to any customer. The federal financial services regulators developed the Interagency Guidance on Response Programs for Unauthorized Access to customer Information and Customer Notice ("Interagency Guidance"), which requires financial institutions to: (1) identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and (3) assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

The FTC's Safeguards Rule, which covers "financial institutions" as defined under GLBA but which is not otherwise subject to regulation by the federal financial regulators, requires institutions to develop, implement, and maintain an information security program that contains the following elements:

- Designate an employee or employees to coordinate the information security program;
- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information (including employee training, information systems management, and efforts to detect and prevent attacks, intrusions, or systems failures);
- Design and implement information safeguards to control the risks through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures;
- Oversee service providers (including requiring service providers by contract to implement and maintain sufficient and appropriate safeguards); and
- Evaluate and adjust the information security program in light of ongoing testing and monitoring of the program.

We therefore recommend to the Task Force that any national data security standards should be based generally on the principles adopted in GLBA and by the FTC's Safeguards Rule, as outlined above, and should further provide that industry sectors already subject to and in compliance with existing requirements would be deemed in compliance with such a national standards. We are concerned that the Task Force's Interim Recommendations, released on September 19, 2006, appeared to reject the idea of providing "safe harbors" for compliance with data security requirements, seemingly ignoring the well-established public policy principle that providing appropriate safe harbors can be an effective way to encourage compliance with such standards while preventing duplicative requirements and regulatory burdens. However, given the breadth of existing data security protections required by federal law in certain industries, imposing additional requirements on these industries would be extremely burdensome and would not provide any additional benefit to consumers of such industries' goods and services. Finally,

there is ample precedent for the use of safe harbors at both the federal and state level (in particular, most state data security laws enacted the past two years has some form of safe harbor) – a fact that the Interim Recommendations ignored and the Task Force should re-evaluate.

The Task Force should examine the recent Congressional record on data security legislation with respect to the establishment of national data security standards and the appropriate use of safe harbor mechanisms in legislation. For example, each of the five principal data security bills reported from the appropriate committees of jurisdiction during the 109th Congress (i.e., H.R. 3997, H.R. 4127, S. 1326, S. 1408, and S. 1789) contained "safe harbor" provisions to ensure that companies already subject to, and in compliance with, existing federal data security regulations and requirements – whether under GLBA, FCRA, or the Health Insurance Portability and Accountability Act (HIPAA), as applicable – were not burdened with additional and potentially duplicative new requirements, but were deemed in compliance with those to be provided by such bills, if enacted.

Additionally, the Task Force should examine the recent record of 35 state data security breach notification laws, nearly all of which have been enacted in the past two years. The overwhelming majority of such state laws contain language deeming entities subject to, and in compliance with, various data security and notification standards to be in compliance with the provisions of the state law.[2] Similar to the federal bills proposed in the 109th Congress, these enacted state laws recognize that the federal regulators of a particular industry are in the best position to evaluate how sensitive consumer data are used, stored, secured and otherwise protected by that industry. This approach also demonstrates a rejection by the states of imposing duplicative and unnecessary new regulations on entities already subject to comprehensive data security and breach notification requirements.

We furthermore recommend that, in addition to supporting similar "safe harbor" provisions for entities in compliance with existing laws, the Task Force consider the commonplace situations in which a breach of data security should not require customer notification, specifically where the data potentially acquired by an unauthorized individual as a result of such breach of security is either publicly available or has been rendered unreadable or unusable by technological or other means. These principles are further explored below in comment I.4 covering breach notification requirements.

4. Breach Notice Requirements for Private Sector Entities Handling Sensitive Consumer Information

Necessity of Uniform, National Standard

The Coalition strongly supports legislation that would establish a national, uniform standard for notification of consumers in the event of a data security breach involving sensitive personal information related to them and that may result in the consumer becoming a victim of identity theft. Consumer notification is not only necessary to provide potentially at-risk consumers with sufficient warning and time to take precautions to protect the misuse of their identities, but uniform rules would also provide businesses and other organizations with greater

[2] *See, e.g.*, California, Delaware, Florida, North Carolina, Ohio, Pennsylvania, Rhode Island, Vermont.

certainty as to their consumer notification responsibilities in the event of a data security breach. Although 35 state laws have been enacted to address data security breach notification (and there are similarities in approach among them), these laws also differ in many material respects from one another, and ultimately create a complicated patchwork of requirements with which companies must comply (thereby causing delays while also raising notification costs) without providing any additional benefit to consumers who are notified.

Breach Notification Trigger

A national, uniform standard for breach notification, if adopted by Congress, should clearly establish a risk-based consumer notification trigger, to eliminate the possibility of over-notification of consumers who are not at risk of harm. In order to implement such a standard, legislation should require that any entity with consumer data that suffers a security breach should first conduct an investigation into the incident to determine the potential risk of identity theft that may result from unauthorized acquisition of consumer data. Additionally, to the extent that such risks can be established, consumers should then be notified as soon as practicable and provided information about the breach and recommendations as to how they may mitigate the potential risk of identity theft. To this extent, we recommend the Task Force review the types of disclosures already required under state data security breach notification laws and proposed in federal bills in the 109th Congress.

A federally-defined and enforced notification trigger that provides discretion to businesses to evaluate the facts and circumstances of a particular security breach incident, on a case-by-case basis, in order to determine the potential risk to affected consumers is a principle that has been endorsed by the Federal Trade Commission as well as numerous proposed federal bills. Such a threshold requirement would ensure that consumers are notified when they actually face a potential harm as a result of breach, and not unduly notified when there is very little likelihood of harm, which would cause unnecessary alarm.

The importance of recommending legislation that requires a risk-based notification trigger has been highlighted by the recent experience by businesses complying with state data security laws. This experience has shown that there are numerous situations in which a data security breach may have technically occurred, but realistically there is no threat of identity theft.. For example, if a misplaced laptop containing unprotected sensitive personal information is obtained by an unauthorized individual, but is recovered before the data is actually accessed, copied, or transmitted, a "breach of security" has technically occurred under the definition used in many state laws, but there is no possible threat of harm to any affected individual. Notification to them would serve no practical purpose or any legitimate public policy interest. Similarly, if an unencrypted magnetic tape used to back up database files has been lost in transport but the files can only be read by a very costly and proprietary machine, there has been a breach of security surrounding that data, and many state laws would require notification in this instance despite the reality that there is a very low likelihood that anyone who acquires the tape (other than the company that owns the proprietary machine) could actually use the data.

Requiring consumer notification in the event of *every* data breach (defined as every unauthorized acquisition of sensitive personal information) would, we believe, result in over-

notification to consumers and their likely desensitization to future notices of breaches in security that may actually warn them of a real risk of harm. Setting a threshold requirement that a "significant risk of identity theft" be present before notification is triggered, as called for repeatedly by the FTC in Congressional testimony, would help ensure that the purposes of consumer notification are met – in other words, that when consumers receive security breach notices, they can take appropriate action to protect themselves. That is not possible if consumers are inundated with unnecessary notifications, particularly of breaches that may cause them no harm whatsoever. For example, a comprehensive study produced last year by Javelin Strategy and Research (entitled, "The 2006 Identity Fraud Survey Report") determined that, "Of those consumers with known data breaches [via notification], the percentage that suffers fraud is only 0.8%."

Implementing such a risk-based threshold requirement for notification also combats the false perception that data breaches are causing more incidents of true identity theft. The number of *reported* data breaches is increasing, but the increase is in large part due to companies focusing more attention on the issue and having to comply with a multitude of state laws requiring consumer notification. An increase in the number of reported data breaches therefore does not indicate whether the number of instances of identity theft has increased year-over-year.

Similarly, the *New York Times* in an article published on September 27, 2006, reached the same conclusion as the Javelin study after analyzing the relationship between reported data breaches and actual instances of identity theft. The article stated, "[W]hile high-profile data breaches are common, there is no evidence of a surge in identity theft or financial fraud as a result." In the *New York Times* on the same date, Fred Cate, a well-known specialist on privacy and security issues, also commented that "The threat of identity theft from data losses is being greatly exaggerated...[a] lot of people have fallen into the trap of equating data loss with identity theft." Providing empirical data for this observation, the Javelin study had found that very often identity theft is perpetrated by someone close to the individual, such as a family member or friend who has ready access to sensitive personal information, and that lost or stolen wallets, checkbooks, or credit cards are the main source of theft of personal information when the victim can identify the source of the data compromise.

The Javelin study concluded that perpetuation of the unproven (and largely anecdotally driven) presumption that data security breaches routinely lead to identity theft is a disservice to consumers. These consumers may be swayed by the alarmist warnings of the media and inundation of breach notification letters into freezing their credit files (limiting their ability to readily obtain credit), canceling credit and bank accounts, or purchasing credit insurance or credit monitoring services at their own expense, which may ultimately be unnecessary. As the study simply stated, "The fear that is being generated is out of proportion to the resulting fraud, which is minimal".

The Task Force should therefore consider all of this recently reported data and analysis in assessing the relationship between the instances of reported data breaches and those of actual identity theft that may result. Additionally, in any recommendations regarding breach notification legislation it may make, we suggest that the Task Force carefully consider the conditions under which the government may require when notifications should be made in order

to ensure not only that there is a legitimate public policy interest being served by such notice but also that there is no unintended harm that may occur due to overbroad notice requirements.

Notice to Individuals

Another factor that should be considered as part of any recommendations regarding an effective notification regime is to whom notice should be made in the event of a security breach. For example, the previously mentioned Interagency Guidance provides that notification of a breach need only be made to *individuals* that are customers, and not to *businesses* or other entities that are customers. Specifically, the Interagency Guidance "does not apply to information involving business or commercial accounts. Instead, the final Guidance applies to nonpublic personal information about a 'customer' ... namely, a consumer who obtains a financial product or service from a financial institution to be used primarily for personal, family, or household purposes, and who has a continuing relationship with the institution."[3]

The need for such limitation has become obvious in industry's recent efforts to comply with state data breach notification laws, which typically fail to delineate between individuals and businesses. This overly broad application of a notification standard that includes notification to businesses that are customers, instead of simply customers that are individuals, has resulted in increased compliance costs that do not serve the purposes for which notification is required. For example, entities serving small businesses must often undertake extensive investigation (including additional information collection), following a breach of security affecting their customers, in order to determine if any persons "related" to such small business customers may have guaranteed loans or other debt, or may have been involved in some other way with the business, and must now be notified of the breach (even though they are not technically customers of the entity and their data may not be at risk). Therefore, any policy recommendation regarding federal breach notification legislation should also include a recommended limitation on requiring breach notification to be made to affected individuals alone, as in the Interagency Guidance. Such a limitation, if implemented, would afford a federal regime with a more narrowly tailored and sensible public policy regarding breach notification than some state laws that have had the unintended consequence of forcing unnecessary investigation by breached entities into their small business customers' operations simply to ensure compliance with overly broad notice standards. It would also have the benefit of being consistent with existing federal breach notification guidance, as noted above.

Covered Data

In addition to the questions of "when" and "to whom" breach notification should be made, we suggest that any recommendations for legislation must recognize that there are certain categories of information that should not trigger notification, even if such information is acquired in a data security incident. These categories of information should be excluded from the definition of "covered data" that is subject to breach notification under any proposed legislation[4],

[3] *See* "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," 12 C.F.R. §30.

[4] Please note that while these recommended exclusions of certain data from the definition of "covered data" may also be refereed to as "safe harbors" by others, these comments have already used the term, as more commonly used

and include publicly available information from government sources, as well as information that has been rendered unreadable or unusable in the event of unauthorized acquisition. A note on each of these two categories follows:

- *Publicly available information*: The trend in state laws is to exclude from the definition of "covered data" information that is publicly available from federal, state or local government records or widely distributed media (*See* previously enacted data security breach notification laws of the states of Arizona, Colorado, Connecticut, Delaware, Florida, Idaho, New Jersey, and Ohio). Additionally, recently enacted state laws have continued to broaden this exclusion, exempting information in the public domain regardless of its source (*See* enacted laws of Utah and Vermont), because there is no practical reason to treat the information as private where it is readily available to the general public through legitimate avenues.

- *Information unreadable or unusable*: Several states currently exempt from the definition of "covered data" information that cannot be used to commit identity theft because, as the Arizona statute states, it is "encrypted, redacted, or secured by any other method rendering it unreadable or unusable." *See* Ariz. Rev. Stat. § 44-7501 The states of Colorado, Connecticut, Nebraska, Ohio, and Utah have also adopted similar standards. These more recent state law approaches reflect the reality that there are various ways to protect personal information, both technologically-based methods as well as ones that may be accomplished with little or no additional technological resources (e.g., masking, redaction or truncation of account numbers).[5] Additionally, the public policy justification for excluding such information from the definition of covered data is that data that has been rendered unreadable or unusable presents no risk of identity theft (even when potentially acquired by an unauthorized person), and therefore consumer notification following a breach of such data is unwarranted.

Key Definitions

Another key aspect to ensuring not only the development of uniform national notification standards, but ones that truly are aimed at reducing identity theft, are recommending definitions that are narrowly tailored to cover the type of information that could be used to by criminals to commit identity theft in the first place. The most important definitions that the Task Force should consider include the definition of what constitutes "personal information" for purposes of notification, as well as the very definition of what constitutes "identity theft" if such term is to be used in connection with a risk-based notification trigger. Each of these terms will be addressed separately below.

---

in proposed federal data security legislation to date, for provisions that deem compliance with the legislation for any entities in compliance with existing federal data security laws, such as GLB or HIPAA. For clarity and consistency within these draft comments then, the term "safe harbor" is used for that connotation only, and not these exclusions.

[5] Flexibility in the means of rendering data unusable affords businesses the ability to choose among alternatives that vary significantly in cost, a factor that may be more important to cost-conscious businesses that must protect data.

- *Definition of "Personal Information"*: Most state laws have followed California's lead with respect to what data should be considered covered data for purposes of providing consumer notification in the event of a security breach. This is often accomplished in state legislation (as well as in proposed federal legislation) through the definition of "personal information." Subject to certain carve-outs for the rendering of information unreadable or unusable via encryption, redaction, truncation or other such methods (as discussed above), nearly all of the 35 state breach notification laws narrowly define the term "personal information" as the combination of an individual's name with any one of the following three categories of data elements: 1) SSN, 2) state driver's license number (or, alternatively, a state identification number), or 3) a financial account number, including a debit or credit card number or other account number, including any password, pass code, PIN or other security factor necessary to access such financial account. The public policy consideration behind such a definition has been to narrowly tailor it to cover the kind of personal information that could be used to commit identity theft against an individual if acquired by an unauthorized person following a breach in security. We recommend that the Task Force not recommend any policies that would broaden this definition to include other kinds of information that cannot be so used to commit identity theft. We also strongly caution against the use of "catch-all" clauses that would permit the ongoing expansion of the definition beyond the parameters that have proven to be suitable to achieve the public policy aims of notification at the state level, as well as proven workable for businesses suffering breaches that must comply with such notification standards.

- *Definition of "Identity Theft"*: Depending on how federal legislation for security breach notification standards is drafted, defining the term "identity theft" may not be necessary. However, as we have previously recommended, we believe, the Task Force should adopt a notification trigger standard requiring that a "significant risk of identity theft" be found before consumer notification is required. Because of this recommendation, we necessarily want to be clear what we mean by the term "identity theft" for these purposes. Simply stated, we believe the term should be drafted to clearly include the type of pernicious fraud that occurs when personal information (as defined above) is used without authorization as false identification for the purpose of opening new financial accounts in that individual's name in order to defraud the individual and the business in which the account is opened. Additionally, we believe the term "identity theft" should not include conduct that actually constitutes "credit card account fraud," or the type of fraud perpetrated by using an existing credit card number to make purchases of goods or services. These latter cases of credit card fraud have already been addressed by criminal statute, law enforcement at all levels of government, as well as industry efforts for many years. In fact, credit card issuing banks and credit card networks bear nearly the entire cost of such fraud. Rather, the Coalition believes that the Task Force should recommend that Congress redefine "identity theft" to refer to the term commonly understood by both consumers and businesses alike.

Federal Enforcement Regime

To establish an effective, multi-layered federal enforcement regime of any proposed legislation, the Coalition recommends that the Task Force endorse a regime that would provide for enforcement of federal laws at the federal level – specifically, a regime where financial institutions are under the enforcement authority of their functional federal regulator and the FTC enforces the law for non-functionally regulated companies. Additionally, the Coalition recommends that such legislation not be enforceable by state attorneys general, as such enforcement within states may lead to uneven application and interpretations of the federal law's provisions based simply on geographic location. Rather, we recommend that the Task Force consider the use of U.S. Attorney Offices to enforce the law under the direction of the U.S. Attorney General and the Department of Justice. Not only do U.S. Attorneys outnumber state attorneys general – thereby providing greater coverage of the United States on a per capita basis – but they also have the benefit of being federal enforcement authorities under the direction of the U.S. Attorney General, who is better situated to enforce any federal data security law more evenly throughout the United States than would 50 different state attorneys general. Finally, the Coalition recommends that the Task Force reject private rights of action as a mechanism to enforce data security safeguards and breach notification legislation, similar to the majority of the congressional committees that reported federal data security bills in the 109th Congress. As FTC Chairman Majoras has testified, no data security solution is perfect, and data security breaches are inevitable despite the best efforts of industry or government to protect against it. That reality means that law enforcement must exercise discretion, looking at the facts of each case, in order to determine when a violation has truly occurred.

5. Education of the Private Sector and Consumers on Safeguarding Data

The Coalition believes that the Task Force should focus on evaluating existing educational programs and industry initiatives aimed at protecting information and responding to data breaches because of industry's expertise in this area. As discussed in greater detail in our comments under section II below, industry (in addition to government) is also taking a lead in educating consumers about monitoring their credit and responding to potential threats of identity theft. There is clearly an incentive to continue this effort, as consumers consider companies' record of safeguarding information when purchasing goods and services. Industry also has an incentive in the broader marketplace to assure consumers that their online commercial activities are safe. We recommend that any new educational efforts proposed by the Task Force recognize the data security educational initiatives that have already been undertaken in both the public and private sector to inform consumers of the various steps they may take to protect themselves against becoming victims' of identity theft, and the benefits and costs of each of those alternatives.

6. Government Receipt of Technologically Secured Data

An additional step government could take would be to improve the security of personal information it collects from the private sector associated with customer data. We believe that the Task Force should recommend that any government department or agency that receives sensitive customer data from the private sector require and implement the use of technologies that would

enable it to receive such data in encrypted form or in other commonly used and technologically protected forms or methods. For example, the federal government regularly requires financial companies to submit confidential customer information to government agencies for various purposes. Often, companies are required to decrypt protected data for transmission to government because it does not have the technological capability to receive the data in encrypted form or other protected method. Therefore, the information is put at much greater risk of misuse at the request of government; a risk that could be avoided simply by closing the government's technological gap. Ensuring that government agencies and departments can receive data from the private sector in a form that maintains its security in transmission would be a critical step in reducing the vulnerability of protected data used by government.

II. PREVENTING THE MISUSE OF CONSUMER DATA

The Task Force is seeking comment on how it might make it more difficult for identity thieves to use consumer data to steal identities after they have successfully obtained such data, for example by recommending to the President that authentication methods be used to prevent the opening of new accounts or access existing accounts of consumers. The Task Force also seeks comment on whether any other measures (beyond authentication) should be considered to prevent the misuse of consumer data by unauthorized individuals once obtained.

We are concerned by this inquiry and by the Task Force's Interim Recommendations because it does not seem to adequately recognize the extent to which private industry is already acting extensively – often voluntarily and without government mandate – to prevent identity theft and other misuses of consumer data. Collectively, industry has and continues to commit hundreds of millions of dollars to these efforts.

The Task Force should also recognize that recently conducted studies have validated that businesses bear 90% or more of the costs associated with the misuse of consumer data. Businesses, therefore, have powerful economic incentives – in addition to consumer service and brand incentives – to reduce identity theft and other fraudulent use of consumer information.

The incentive for businesses to mitigate identity theft and other fraudulent uses of consumer information is reflected, in part, by the growth of advertisement campaigns that emphasize a commitment to information security. From internet service providers to financial institutions, many companies that use, store, or transmit consumer information have voluntarily implemented safeguards to mitigate fraud. As a means to differentiate themselves from competitors and enhance brand value, it is now commonplace for companies to highlight their information security "best practices" through online, print, and television advertising.

Additionally, recognizing the threat posed by identity thieves and the importance of aggressive efforts to combat the changing nature of the crime, individual businesses and corporate leaders have often joined together in cross-industry initiatives aimed at reducing identity theft and protecting consumer information. These initiatives are not only innovative but also effective at enhancing information security and reducing identity theft. For the Task's Force's benefit, we have included – as separate bullet points – a number of examples at the conclusion of this comment section.

Generally speaking, however, some of the steps taken by corporate America – through individual company efforts as well as through the unified efforts of industry associations – seek to educate consumers and improve how consumers use, store, and share their personal information. In other instances, the private sector has provided financial resources, thought leadership, and executive support to develop internal programs and best practices to safeguard the manner in which information is handled and maintained.

As an example of the collaboration underway, the U.S. Chamber of Commerce (the "Chamber"), in collaboration with Visa and Microsoft, has developed an interactive, web-based Security Toolkit to help business owners recognize data security vulnerabilities and improve their data security practices. In May 2006, the Chamber launched its "Get Net Safe" campaign, a national outreach program that visited twelve American cities to "raise awareness about threats to online security" and educate consumers on ways to "protect themselves and their families." Partners in the Get Net Safe tour included the National Cyber Security Alliance, the Internet Education Foundation, and the AARP.

Industries have also taken steps to promote the introduction and implementation of best practices that improve the manner with which corporate America handles consumer information. For example, the Internet Security Alliance, an organization representing a wide range of businesses, unveiled the publication, "Contracting for Information Security in Commercial Transactions - An Introductory Guide." (Guide). This publication helps businesses address data security requirements that are increasingly necessary in commercial, contractual relationships.

When unveiled in late 2005, the Guide served as one of the first publications to address information security contracting, thereby harmonizing data security practices and reducing the likelihood that personal or other sensitive information will be misused. The initial success and utility of the Guide has prompted the development of a second version, scheduled for release in early 2007. The second version builds upon previous successes and will emphasize information security controls, such as ISO 17799.

Industry has also led in the development of information security best practices. The Internet Security Alliance has also published best practices, such as the "Common Sense Guide for Senior Managers." Companies that implement the best practices can receive a discount on the purchase of cyber insurance. This incentive rewards the implementation of information security best practices and the corresponding purchase of insurance, which transfers the risk of loss that can be associated with information security incidents. Similarly, the National Cyber Security Alliance raises awareness and advances information security by providing timely information and offering useful tools to Internet users. For example, in order for Internet users to assess the state of their own information security practices, the National Cyber Security Alliance's website includes a web-based security self-assessment.

While industry has taken its own initiatives (separate from government involvement or mandate) to make significant strides to raise awareness, develop best practices, and provide resources to prevent identity theft, it is essential that enhanced public-private cooperation also be developed and take root. Forging meaningful partnerships between government and industry to

develop accurate and reliable identity theft statistics, coordinate education and outreach efforts, and develop strategies that reflect the dynamic nature of identity thieves should not only be one of the recommendations of the Task Force but also an ongoing priority of the federal government.

The Task Force should also note that successful public-private initiatives in the realm of cyber and data security have precedent. In December 2003, at the National Cyber Security Summit, the Department of Homeland Security and key private sector participants – including the Business Software Alliance (BSA), the Information Technology Association of America (ITAA), and the Chamber – came together to begin a dialogue on cyber and data security. Nearly three years later, that dialogue has continued – and expanded. In late 2005, industry and government met again to expand cross collaboration to improve information security practices.

The National Cyber Security Summit, and its subsequent successes, represents a model for increased public-private partnership opportunities to address identity theft. Indeed, the development of Department of Homeland Security's National Infrastructure Protection Plan (NIPP), as just one example, illustrates the commitment of all sides to the advancement of common goals and the growth of public-private cooperation.

The June 2006 release of the NIPP marks a milestone for public-private partnerships to protect critical infrastructures, including their cyber components. As Department of Homeland Security Under Secretary for Preparedness George Foresman stated, "[t]he NIPP is the path forward on building and enhancing protective measures for the critical infrastructure assets and cyber systems that sustain commerce and communities throughout the United States…[t]he NIPP formalizes and strengthens existing critical infrastructure partnerships and creates the baseline for how the public and private sectors will work together to build a safer, more secure and resilient America."[6]

To coordinate public-private efforts to secure the physical and cyber components of the nation's critical infrastructure, each critical infrastructure sector developed a Sector Coordinating Council (SCC). Cyber security has been a key topic among SCCs as they work with the government to enhance homeland security and implement the policy goals outlined in the NIPP.

As previously noted, in order to provide the Task Force with a summary of the notable involvement of our member companies and organizations to prevent identity theft and other fraudulent use of consumer data, we have provided the following bullet point summaries of initiatives which we recommend the Task Force consider in developing its recommendations to the President. We also request that the Task Force's summary report specifically recognize such efforts to highlight the steps voluntarily underway by industry to combat identity theft:

- Many mutual fund companies:
    - Do not accept convenience checks, money orders, or third-party checks to open accounts since those forms of payment are too easily negotiated by thieves;

[6] Press Release, Department of Homeland Security, DHS Completes National Infrastructure Protection Plan, (June 30, 2006), *available at* http://www.dhs.gov/xnews/releases/press_release_0940.shtm.

- Require two factor authentication whenever a shareholder wants to transact business by phone or computer;

- Send dual confirmations when shareholders change their address of record on an account; the mutual fund company sends one confirmation to the old address and one to the new address to make sure the shareholder is, in fact, initiating the change. Similarly, when a shareholder changes the bank of record on an account they confirm the change in writing to the customer. Some funds also limit, for a specified period of time, a shareholder's ability to have funds transferred to a new bank of record to enable the fund to verify the banking information;

- Limit access to non-public personal information held by their organizations to necessary personnel;

- Monitor, pursuant to SAR requirements, suspicious activity in shareholder accounts;

- Regularly monitor websites for phishing and firewalls for hacking;

- Include information on their websites and in their printed communications to investors alerting them to ways to protect themselves against fraudulent behavior; and

- At least one fund company has agreed to reimburse investors for unauthorized activity in their investors' accounts.

- Many financial services firms:

  - Perform assessments of network security to determine the adequacy of protection from intrusion, viruses, and other data security breaches. Identified weaknesses are addressed through implementation of additional hardware and software, and modified user procedures, as appropriate;

  - Post identity theft education materials available to customers *and non-customers* on company websites. Tips include steps to protect personal information online, ways to prevent fraud and identity theft, and ways to report fraud;

  - Implement systemic and manual controls in production processes to alert for potential identity theft; and

  - Formed an inter-association committee to serve as a conduit for member companies to join forces to deter, detect, and prevent fraud. The committee shares best practices concerning security standards and data safeguarding, exchanges information about proactive detection and investigation techniques,

develops consumer and industry fraud awareness initiatives, and created an early warning system for new fraud threats emerging in the U.S.

- Many securities firms:
    - Publicly advocated for the implementation of data breach notification rules by the Securities and Exchange Commission and other functional regulators under GLBA; and
    - Work to increase industry awareness of identity theft issues and coordinate with regulators and law enforcement on account intrusions, for example, in instances of account misuse.
- Through unique products and services, individual companies help secure information and reduce identity theft. For example:
    - Companies within the consumer data industry offer services which provide companies comprehensive background checks on prospective employees and tenants as permitted by law under the Fair Credit Reporting Act. They also help companies verify the identity of prospects and customers, help law enforcement locate criminals, and provide access to other vital information to improve company processes to detect and prevent fraud.
    - A leading payment processing and bill payment company recently deployed an automated fraud detection and case management system to more than 40 financial institutions. The system helps ensure that receiving and paying bills online remains safer than doing so offline with paper-based bills and checks. To mitigate risk and reduce fraud for banks and consumers before it happens, the system combines the company's cumulative knowledge of payment patterns and a sophisticated analytics engine to help financial services organizations detect and stop unauthorized payments.
    - When a major consumer lending institution encountered a problem when the loss ratio on many of its loans – including mortgages and consumer loans – became excessively high due to fraud, the bank hired a leading provider of fraud prevention products to authenticate potential customers during the application process prior to extending credit. The result was immediate and material: two million dollars of confirmed fraud losses were averted within the first six months of implementation.
    - When an online retailer became the target of an elaborate fraud ring, the company looked to one of the major credit reporting agencies. By using shared data maintained by that agency, the retailer was able to identify applications with common data elements and flag them for "priority status." In the case of this fraud ring, $26,000 in fraud was averted by using shared application data.

III. VICTIM RECOVERY

1. Improving Victim Assistance
2. Making Identity Theft Victims Whole

(Below are the Coalition's collective comments to both Questions 1 and 2 of Section III)

The Interim Recommendations of the Task Force recommended that the Congress amend existing law to allow for the victim of identity theft to seek restitution from the perpetrator of such theft. In the abstract, this recommendation makes perfect sense, but it is too simplistic. The perpetrators of true identity theft are all too often judgment-proof, so where is the restitution to come from? The Interim Recommendations also suggest that part of the restitution should take the form of damages based on the "time" required for the victim to cure the consequences of true identity theft. But it does not say or even suggest how this might be done, other than to place an estimate on the average time spent attempting to cure the problem.

The Coalition endorses the principle of restitution, and we urge the Task Force to include among its recommendations one which brings that reality closer to effect. The Task Force should also recognize that the companies and other entities from which data is stolen are also victims of a criminal act. Additionally, the occurrence of a data security breach, even when no consumers are actually endangered and/or harmed as a result of it, is still a blemish on the reputation of the corporate brand, even if such corporation employed best practices in securing the security of the data. While we support the principle of restitution for victims, the Task Force should recognize that there are often multiple victims of these crimes, and that any business entity that is a victim of a security breach, whether by fraud or otherwise, is still a victim of the same crime and should not be looked to as the "corporate deep pocket of last recourse" in the likely event that restitution cannot be made by the perpetrator of the crime.

3. National Program Allowing Identity Theft Victims to Obtain an Identification Document for Authentication Purposes

No comment.

4. Gathering Information on the Effectiveness of Victim Recovery Measures

The Coalition believes the Task Force should recommend that the agencies with enforcement authority for the Fair and Accurate Credit Transaction Act (FACT Act) amendments to the Fair Credit Reporting Act (FCRA) undertake a joint agency study to assess the impact and effectiveness of the FACT Act. The Coalition additionally notes that the FACT Act has only been in effect for several years, and that any such analysis should be completed before any policy recommendations are made by the Task Force to further amend FCRA or create additional laws to address any provisions of the FACT Act that the government study reveals have been ineffective in achieving the purposes for which those provisions were originally enacted by Congress.

IV. LAW ENFORCEMENT: PROSECUTING/PUNISHING IDENTITY THIEVES

1. Establish a National Identity Theft Law Enforcement Center

If the Task Force chooses to recommend the establishment of a National Identity Theft Law Enforcement Center, the Coalition recommends that the Task Force consider requiring such a center to incorporate methods of reducing jurisdictional concerns with respect to enforcement of identity theft laws. From an international standpoint, such a center could serve as a resource for domestic law enforcement agencies facing identity thieves in foreign jurisdictions, including nations known for being havens for financial crimes. Additionally, such a center could promote collaboration among domestic law enforcement agencies to ensure cooperation and aggressive prosecution of identity thieves.

2. Ability of Law Enforcement to Receive Information from Financial Institutions

No comment.

3. The Investigation and Prosecution of Identity Thieves Who Reside in Foreign Countries

The Task Force is seeking comment on whether it should recommend to Congress that it amend the provisions of two statutes – 28 USC 1782 and 18 USC 2703 – in order to "clarify which courts can respond to appropriate foreign requests for electronic and other evidence in criminal investigations, so that the United States can better provide assistance to foreign law enforcement in identity theft cases." We recommend that any endeavor to amend the laws of the United States to provide assistance to foreign entities in their own efforts to combat identity theft, that the United States require the foreign entity to provide reciprocal assistance to the United States (as Congress failed to require in the recently enacted US SAFE WEB Act).

4. Prosecutions of Identity Theft

This portion of an earlier draft of the strategic plan being considered by the Task Force suggests mandating the creation of an identity theft coordinator in each U.S. Attorney's Office, and the federal government's formal encouragement of state prosecutions of identity theft, with "working groups" and "task forces" created to focus on the swift and efficient prosecution of these crimes. While the goal is, of course, laudable, it may not be necessary to mandate that every US Attorney's Office in the country have such a capacity. True identity theft, in which a consumer's identity is stolen by another for the purpose of opening an account or establishing themselves as the consumer, is not as widespread as some policymakers believe. It may well be that U.S. Attorneys can make better use of their finite resources to address the violations of law taking place most often in their jurisdictions. It is the individual offices, and not the Congress nor the Task Force, that are in the best position to administer the resources allocated to the U.S. Attorney's Offices, and when there is an expressed need to follow recommendations of this kind,

then the applicable U.S. Attorney's Offices should have access to the funding and the personnel necessary to protect the residents of their districts.

We also take the view that federal litigation authority ought to broadened to include the right of the U.S. Attorney General to appear in federal court for the purpose of prosecuting crimes of this kind, both criminally and civilly. At the moment, the Attorney General has no such right, and the FTC is the lead agency. If true teeth are to be placed into reducing identity theft, federal prosecutions have to have recourse to civil as well as criminal remedies.

5. Targeted Enforcement Initiatives

A key concern about the sale or transfer of SSNs arises when the entity obtaining the SSNs uses unfair or deceptive means to obtain the SSNs, often for the purpose of selling those SSNs for illegitimate or unlawful purposes. Financial institutions under GLBA have a clear obligation to know the entity to which they are transferring SSNs, and they undertake sufficient due diligence efforts to ensure that the recipient is obtaining the SSNs for a legitimate and lawful purpose. This effort ensures that the SSNs are not transferred to and subsequently offered for sale by bad actors. Such a standard is easily applicable to non-financial entities that may possess SSNs; in fact, the FTC's settlement with ChoicePoint demonstrates the Commission's ability under current law to enforce such a standard. Entities that use unfair or deceptive means to obtain SSNs should be prosecuted fully under the law.

We believe it is therefore unnecessary for the Task Force to recommend any new or "special" targeted enforcement initiatives focused exclusively or primarily on unfair or deceptive means to make SSNs available. The Task Force must recognize that the illegitimate sale of SSNs is only one aspect of the much broader concerns with preventing identity theft and that the federal government must make appropriate resource allocation determinations that will have the greatest impact in reducing the likelihood and prevalence of identity theft on the greatest number of individuals. We are not aware of any substantial empirical evidence indicating that a majority of compromised SSNs used for identity theft purposes can be traced back to unfair or deceptive practices to make SSNs available, as there appear to be other legal as well as illegal sources for obtaining SSNs, such as through review of records made available by government entities, computer hacking, dumpster diving and outright theft of laptops and computers containing such data. The Task Force should therefore take into account to what extent unfair and deceptive practices to make SSNs available is a source of the identity theft problem, and marshal its resources appropriately.

We recommend that, as noted above in comments I.1 and I.2, the Task Force recommend a comprehensive study that fully examines the societal benefits of the legitimate uses of SSNs and augment such analysis with a review of the illegitimate uses of SSNs, including the extent to which unfair deceptive acts and practices are being used to offer them to the general public, as well as the impact such activity (in relation to other activities) is or may be having on the amount of identity thefts suffered. If one of the Task Force's principal objectives is to better understand the uses of SSNs and whether additional protections can be instituted to further protect the integrity of SSNs, that understanding should necessarily come before any attempts at specialized

enforcement initiatives that may have no effective impact on reducing the amount of identity theft suffered by consumers.

6. Amendments to Federal Statutes and Guidelines Used to Prosecute Identity Theft Related Offenses

Proposed Amendment to 18 U.S.C. § 1030(a)(5)

The Coalition is concerned with the Task Force's recommendation that Congress pass legislation to eliminate the damage and loss requirements from section 1030(a)(5) of the Computer Fraud and Abuse Act (CFAA). Without actual language from the Task Force to review, however, the general description of the proposed change in the comment request notice is a cause for concern on the part of legitimate businesses that install software on consumers' computers or otherwise access consumers' computers in order to provide business goods or services to them at their request.

Although consumers can typically be construed to have given "implied consent" to the accessing of their computers and/or the use of software on their computers in order to receive goods and services, it is unclear (without further explanation by the Task Force) whether the proposed amendments it is considering to the CFAA would deem such implied consent to be sufficient authorization (and therefore outside the scope of section 1030(a)(5)). If not, the use of such legitimate business software and the access to information on consumers' computers by commercial entities, as commonly occurs today, may be "without authorization" under the terms of the CFAA. Without further damage or loss requirements, however, such commonplace computer software or access for online businesses would *alone* constitute a federal crime unless the consumer had granted affirmative consent (not an implied consent) to such activities. We presume that the Task Force is not intending by this proposal to effectively turn section 1030(a)(5) into a criminally enforceable opt-in statute for the currently lawful accessing of a consumers' computer, or use of software on it, in order to provide them with online goods or services, but it should be clarified by the Task Force nonetheless.

The impact of such a change in the law could be enormous, as businesses engaged in e-commerce retract from offering online goods or services for fear of conducting online business under such broad federal criminal liability standards. For example, this proposed amendment would, on its face, ostensibly create criminal liability even for businesses that currently use security software on consumers' computers to prevent fraudulent transactions (such anti-fraud software is often placed on consumers' computers by online businesses without a consumers' affirmative consent so as not to tip-off would-be "fraudsters" as to how they might work around or disable such anti-fraud mechanisms). The Task Force should also understand that, before making such a far-reaching proposal, these concerns do not arise for legitimate businesses under the current statutory language of the CFAA. That is because the current damage and loss requirements (which the Task Force is considering eliminating) now work together to protect legitimate, commercial behavior from the broad reach of the CFAA because it would be unlikely that any such legitimate commercial behavior would damage a computer and/or cause losses in the amount $5,000 or more.

For these reasons, we strongly recommend that the Task Force reconsider the currently proposed amendments to section 1030(a)(5) of the CFAA, and that it seek alternative methods to address what it has termed "malicious spyware," especially given that the current language of section 1030(a)(5) is not limited to such spyware. As the Task Force may already understand, section 1030(a)(5) is not a spyware provision at all, but applies broadly to any intentional accessing of a consumers' computer or transmission to it of "a program, information, code, or command." Therefore, if the Task Force were to recommend the proposed amendment as described in the comment request notice, it would not be limited to affective purveyors of spyware alone, but, rather, could result in a change in the CFAA by which all legitimate businesses, across multiple industries, that provide online goods and services to consumers are potentially criminally liable for conducting the very online activities they perform today for lawful commercial purposes. In fact, a counter-intuitive result that could follow from the Task Force's proposed amendment to CFAA, if enacted, would be that consumers who purchase goods or services online from lawful businesses, and therefore impliedly consent to the access or use of software on their computer to complete such transactions, may find in the future that such goods and services are no longer available online.

7. Training for Law Enforcement Officers and Prosecutors

No comment.

8. Measuring Law Enforcement Efforts

While the Task Force has proposed a number of surveys and studies to conduct, we recommend it recommend further study on the following questions:

- Measurable Correlation Between Breaches and Instances of True Identity Theft: The Task Force should recommend a study to determine the extent to which breaches of data security have actually resulted in instances of identity theft (defined as the establishment of new accounts by fraudulent means through the misuse of personal consumer information obtained as a result of the security breach);

- Sources of Personal Data Used By Identity Thieves, Including Legally Available: The Task Force should recommend a study to determine the extent to which the source of personal information used by identity thieves (where known) was obtained through one of the following means:

    - Data security breach involving criminal intent of the perpetrators (e.g., theft of a laptop, computer hacking, stolen packages with backup tapes, etc.);

    - Data security breach occurring as a result of business negligence or mishandling of data, including poor data security practices resulting in the unintentional making of confidential personal data public availability;

    - Illegal purchases of SSNs via unfair or deceptive acts or practices;

- Legal reviews of public records made available by governmental entities; and
- Offline methods of gathering such information (e.g., "dumpster diving").

- Prevalence of Over-Notification and Insufficiently High Notification Triggers: The Task Force should recommend a study to determine the extent to which those individuals who have been notified in 2005 and 2006 of data security breaches have actually become the victim of identity theft or suffered any other measurable harm.

CONCLUSION

The Coalition appreciates having the opportunity to provide the above comments. We are available to answer any questions that may arise, and thank you for your consideration of our views.

Sincerely,

/S/

Thomas M. Boyd
Counsel to the Coalition

Alston & Bird LLP
The Atlantic Building
950 F Street, NW
Washington, DC 20004
(202) 756-3372